

STEPHANIE M. HINDS (CABN 154284)
Acting United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

DAVID COUNTRYMAN (CABN 226995)
CHRIS KALTSAS (NYBN 5460902)
CLAUDIA QUIROZ (CABN 254419)
WILLIAM FRENTZEN (LABN 24421)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-436-7428
FAX: (415) 436-7234
claudia.quiroz@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

Approximately 69,370 Bitcoin (BTC), Bitcoin
Gold (BTG), Bitcoin SV (BSV), and Bitcoin
Cash (BCH) seized from
1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx

Defendant.

First 100, LLC, 1st One Hundred Holdings,
LLC, and Battle Born Investments
Company, LLC,

Claimants.

CASE NO. CV 20-7811 RS

DECLARATION OF JEREMIAH HAYNIE IN
SUPPORT OF UNITED STATES' REPLY IN
SUPPORT OF MOTION TO STRIKE THE CLAIMS
OF CLAIMANTS BATTLE BORN INVESTMENTS
COMPANY, LLC, FIRST 100, LLC AND 1ST ONE
HUNDRED HOLDINGS, LLC

Hearing Date: September 9, 2021
Time: 1:30 p.m.
Court: Hon. Richard Seeborg

1 I, JEREMIAH HAYNIE, state as follows:

2 1. I am a Special Agent with the Criminal Investigation Division of the Internal Revenue
3 Service (“IRS-CI”). I am a case agent assigned to this case. I respectfully submit this declaration to
4 provide certain relevant information in support of the United States’ Reply in Support of Motion to
5 Strike the claims filed by Claimants Battle Born Investments Company, LLC; First 100, LLC; and 1st
6 One Hundred Holdings, LLC (“Claimants”). I personally conducted the blockchain analysis of the
7 bitcoin at issue in this case and was involved in the investigation from its inception to the present day. I
8 have been a Special Agent with IRS – Criminal Investigation (IRS-CI) for approximately 19 years.
9 Since 2015, I have been assigned to the IRS-CI Cyber Crimes Unit. I have conducted investigations
10 involving cryptocurrency since 2014 and have traced different cryptocurrencies both manually and using
11 blockchain analytics tools in dozens of cases. In addition, I hold an active Chainalysis Reactor
12 Certification.

13 2. I have reviewed the Opposition to Motion to Strike the Claims of Claimants Battle Born
14 Investments Company, LLC, First 100, LLC, and 1st One Hundred Holdings, LLC filed on August 10,
15 2021. I have also reviewed the supporting declaration of Jacky Lee, a data scientist at DMG Blockchain
16 Solutions retained by counsel for the Claimants to conduct a forensic analysis related to the
17 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx (“1HQ3”) Bitcoin address (hereinafter “Lee
18 Declaration”). Based on my knowledge and experience, including my experience conducting
19 cryptocurrency tracing analysis in dozens of investigations, my assessment of Claimants’ analysis
20 linking the transactions executed by Individual X to files purportedly deleted from Ngan’s computer is
21 that it is flawed and incorrect.

22 3. I personally conducted the tracing and analysis of the 1HQ3 Bitcoin address using the
23 Chainalysis Reactor blockchain analytics software. In addition, my team and I conducted a manual
24 analysis of the 54 bitcoin transactions at issue in this case and compared it against the data from the
25 seized Silk Road servers, which showed a direct link between the addresses from which Individual X
26 stole the bitcoin and Silk Road.

27 4. Nikita Kislitsin is not Individual X.

28 5. Ownership of a particular Bitcoin address can be shown by using the private key to sign a

1 message. Ownership is not established by a screenshot.

2 **A. Individual X Withdrew Funds from Silk Road by Exploiting a Vulnerability**

3 6. On approximately May 6, 2012, Individual X stole 70,411.46 BTC from addresses
4 controlled by Silk Road and transferred it to two Bitcoin addresses—
5 1BADznNF3W1gi47R65MQs754KB7zTaGuYZ and 1BBqjKsYuLEUE9Y5WzdbzCtYzCiQgHqtPN
6 (hereafter “1BAD” and “1BBq”). Individual X used a vulnerability that allowed Individual X to
7 withdraw funds from Silk Road without authorization. A vulnerability is a weakness or opening for
8 hackers to gain unauthorized access to a website, a system that connects to a website, operating
9 systems, web applications, software, networks, or other IT systems.

10 7. Based on a review of the Silk Road seized servers, the transfers to 1BAD and 1BBq came
11 from the general pool of Silk Road bitcoin and not from any particular Silk Road user accounts.

12 **B. Jacky Lee’s Analysis**

13 8. According to his Declaration, one of the tasks Jacky Lee had was to determine “...where
14 the 69,370 Bitcoins in the 1HQ3 wallet came from...” Lee Declaration ¶ 3. Lee determined that it was
15 “highly improbable for an individual to hack 58 wallets that sent Bitcoins to 1HQ3” because “the private
16 key used for accessing bitcoin wallets is very secure and cannot be easily guessed with modern
17 computers.” *Id.* ¶ 17. Lee further determined that it was “impossible for Individual X to gain these
18 Bitcoins by hacking a single silk road wallet[], because the blockchain transactions show that the
19 Bitcoins came from 58 sources.” *Id.*

20 9. By using the vulnerability in Silk Road’s vendor portal as described above, Individual X
21 tricked Silk Road into sending bitcoin to 1BAD and 1BBq. This is not a “far-fetched” or “improbable”
22 scenario, as Claimants characterize it. Many seemingly secure entities such as cryptocurrency
23 exchanges have had cryptocurrency stolen from them. For example, Mt. Gox, the largest cryptocurrency
24 exchange of its day experienced a continuous theft of its bitcoin from 2011 to 2014 resulting in a loss of
25 approximately 850,000 BTC, valued at approximately \$480 million at the time (reuters.com/article/us-
26 bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228). In August 2016, another exchange, Bitfinex,
27 lost 119,756 BTC, valued at approximately \$72 million at the time (fortune.com/2016/08/03/bitcoin-
28 stolen-bitfinex-hack-hong-kong). In May 2019, the CEO of Binance, a large cryptocurrency exchange,

1 announced that hackers executed one unauthorized transaction and withdrew 7,000 BTC valued at
2 approximately \$40 million from Binance's wallet (Binance.zendesk.com/hc/en-
3 us/articles/360028031711-Binance-Security-Breach-Update). These are just three examples out of many
4 instances where an individual or group has been able to gain unauthorized access to seemingly secure
5 systems to steal cryptocurrency. These examples are offered to show that individuals are able to use
6 unauthorized access to transfer bitcoin out of seemingly secure companies.

7 10. Based on my and my team's analysis of the Bitcoin addresses associated with Silk Road,
8 the bitcoin in 1HQ3 did not come from 58 sources and I am unable to ascertain the source of this
9 statement based on Lee's declaration. As described in more detail below, based on my and my team's
10 analysis of the Bitcoin addresses associated with Silk Road, the original source of bitcoin that funded
11 1HQ3 came from 3,056 addresses, 98 percent of which were addresses assigned to specific Silk Road
12 users.

13 11. Bitcoin transactions are not saved in a hard drive as separate files when they take place.

14 12. Lee's company, DMG Blockchain Solutions (hereafter "DMG"), has a blockchain
15 analytics product, called "BlockSeer" that Lee used to analyze 1HQ3. *Id.* ¶ 15. It seems implausible to
16 me that despite its blockchain analytics capabilities, BlockSeer did not identify the 54 transfers as
17 originating from Silk Road, one of the most sophisticated and extensive criminal marketplaces of its
18 time. In fact, based on a Twitter post from @BlockSeer dated December 10, 2015, BlockSeer was
19 aware of Silk Road (*see* <https://twitter.com/blockseer/status/674998974940508160>). According to
20 DMG Blockchain Solutions' website, "Blockseer is an analytics tool that enables the tracking of
21 cryptocurrency on both the Bitcoin and Ethereum blockchains. It examines cryptocurrency flows
22 through wallets" and performs various functions, including "creating private labels and graphs . . .
23 accessing a more extensive list of labels and clusters and additional analytics tools" and "importing and
24 exporting analytics data such as addresses, transactions, and labels."
25 <https://dmgblockchain.com/software-product/>. Despite these purported capabilities, Lee's Declaration
26 and supporting exhibits provide no information about his methodology or any specific findings, charts,
27 or analysis.

28 ///

1 **C. Blockchain Analysis of 1HQ3 Using Chainalysis Reactor**

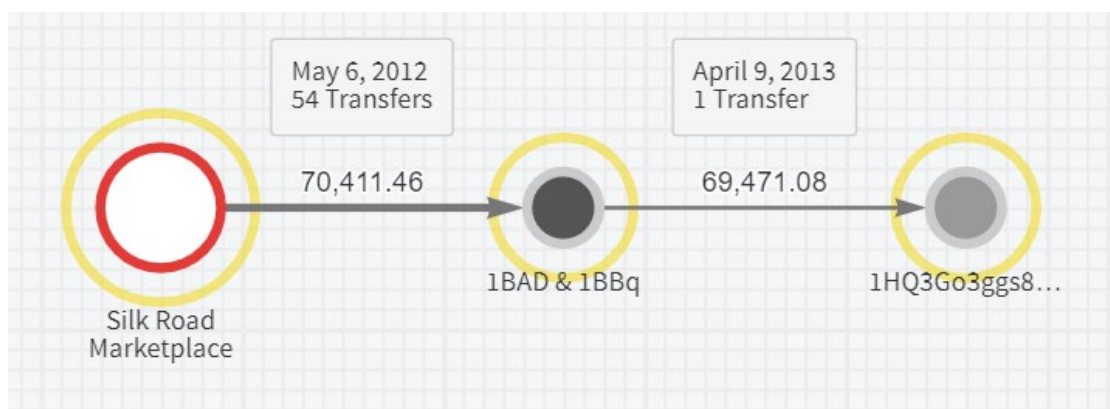
2 13. The majority of cryptocurrency volume flows through services, including legal entities
3 like cryptocurrency exchanges, or illicit ones like darknet markets such as Silk Road. While
4 blockchains contain information on transactions between addresses, they do not provide information on
5 the individuals or entities to which those addresses belong (i.e., who is conducting the transactions).
6 Software analytics companies like Chainalysis conduct proprietary analysis that connect cryptocurrency
7 addresses to real-world organizations by using aggregate data.

8 14. Chainalysis Reactor is an investigative software tool that connects cryptocurrency
9 transactions and addresses to real-world entities such as dark net markets, enabling investigators like
10 myself to understand and interpret activity on the blockchain. Understanding which entities are
11 connected to which addresses requires analytical tools to extract information and methodology to do the
12 matching. Chainalysis maps blockchain transactions to real-world entities by grouping addresses into
13 clusters and identifying those clusters. In simple terms, a cluster is a collection of addresses that are
14 determined by Chainalysis to be controlled by one entity. Chainalysis looks at the history of
15 transactions and runs algorithms to group addresses in a cluster that it determines are managed by the
16 same entity. While Chainalysis generally clusters addresses and labels the cluster according to its
17 category (e.g., cryptocurrency exchange, terrorist financing, darknet website, etc.), they also perform
18 address-level identifications within clusters to name the cluster. Based on this analysis, Chainalysis has
19 identified and labeled a number of entities by name based on the transaction history and other
20 associations. This includes the Silk Road darknet marketplace as well as the two clusters of seized Silk
21 Road funds—one from October 2013 and one from November 2, 2020 (i.e., the seized funds at issue in
22 this case).

23 15. By inputting the 1HQ3 address into Reactor, Chainalysis algorithms automatically
24 created a link between that address and Silk Road, which Chainalysis has identified as a known entity
25 based on a number of factors and data points as well as their algorithms and aggregate data. From this
26 information and my analysis, I was able to determine that the ultimate source of the funds in 1HQ3
27 originated from addresses managed by the same entity: the Silk Road marketplace.

28 16. Attached hereto as Exhibit 1 and replicated below is a graph I created using Reactor to

illustrate the bitcoin transfers relevant to this matter. The series of transactions begins on the left side of Exhibit 1, when on May 6, 2012, Individual X, without authorization, transferred 70,411.46 BTC from Silk Road to two Bitcoin addresses Individual X controlled, 1BAD and 1BBq. The next relevant transaction occurred on April 9, 2013, when Individual X sent 69,471.082201 BTC from 1BAD & 1BBq to 1HQ3.



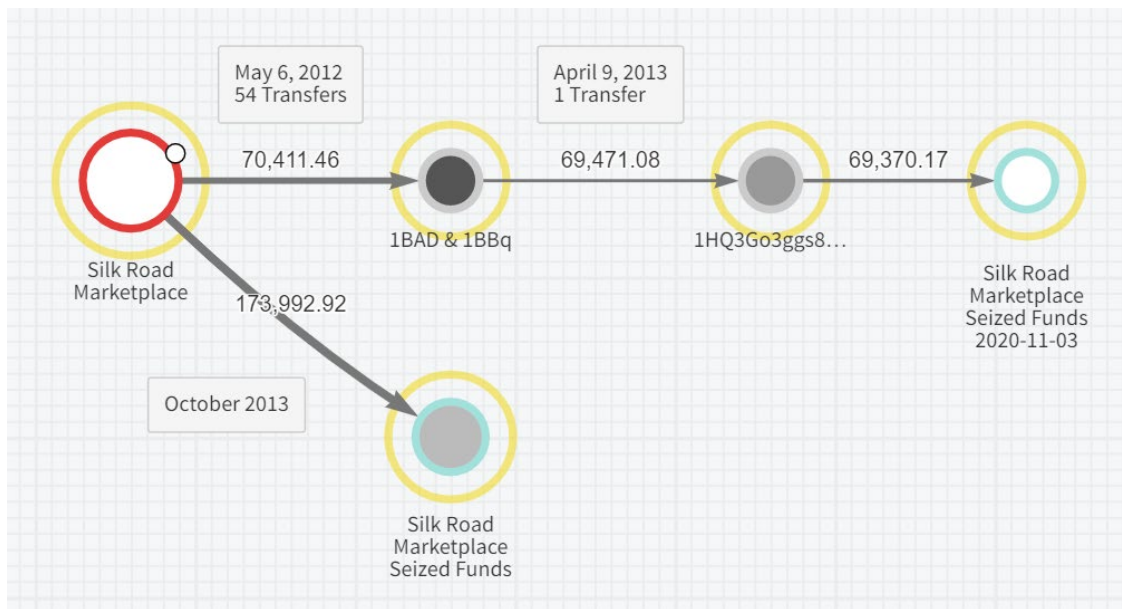
17. As explained above, the references to Silk Road on the chart are not manual inputs by me but rather identifications made by Chainalysis based on the aggregate data and algorithms powering its software.

18. The details of these transfers can be viewed by any member of the public by entering the Bitcoin addresses into a Blockchain Explorer such as Blockchair.com, one of the two websites referenced in paragraph 15 of the Lee Declaration.

19. Attached hereto as Exhibit 2 and replicated below is an expansion of Exhibit 1 that I created using Reactor. Exhibit 2 illustrates that, through its independent analysis, Chainalysis identified and labeled the two seizures of Silk Road funds: (a) the October 2013 seizure by law enforcement and the United States Attorney's Office in the Southern District of New York when the Silk Road website was taken down and Ross Ulbricht was arrested; and (b) the November 3, 2020 seizure by the IRS-CI and the United States Attorney's Office in the Northern District of California following Individual X's consent to the forfeiture of the 69,370 BTC Individual X stole from Silk Road in 2012 to the United States government.

///

///



20. The 173,992.92 BTC depicted in the graph above as “Silk Road Marketplace Seized Funds” in October 2013 consist of 27,618.69843, Silk Road marketplace bitcoins seized during the takedown of the website on October 02, 2013 and the bitcoins seized from Ulbricht’s computer hardware, which were traceable to the operation of Silk Road. I know this based on two things: (1) the number of bitcoins seized from the Silk Road servers on or about October 2, 2013 as detailed in the Southern District of New York’s Notice of Forfeiture; and (2) the number of bitcoins seized from Ulbricht’s computer hardware traceable to the operation of Silk Road with public Key 1FfmbHfnpaZjKFvyi1okTjJJusN455paPH which was seized on or about October 25, 2013 in San Francisco, CA as detailed in the Southern District of New York’s subsequent Notice of Forfeiture.

D. Analysis of Silk Road Servers Seized in October 2013

21. Blockchain analytics using proprietary software is not the only source of information about the origin of the Defendant Property. During the October 2013 takedown of Silk Road, law enforcement seized servers that contained Silk Road transaction data. This data confirmed that the 54 transfers at issue here originated from Silk Road.

22. Although people often use them interchangeably, there is a significant distinction between a cryptocurrency wallet and an address. A wallet is a collection of private keys and corresponding addresses. It is typically under the control of a single private individual or service. An address is a digital destination used to send and receive cryptocurrency funds. It is similar to a physical

1 house address or an email address. Cryptocurrency wallets often contain many addresses. A Bitcoin
2 address is a hash of the public key and consists of 26-35 alphanumeric characters.

3 23. In bitcoin transactions, multiple addresses can be used to fund a particular transaction.
4 For example, if an item costs 5 BTC, but the buyer only had 3 BTC in one address and 2 BTC in another
5 address, the buyer would use the funds from both addresses to make the payment. This is often referred
6 to as a transaction having multiple “inputs” (in this example, two inputs and one output).

7 24. In this case, Individual X sent the stolen bitcoin to 1BAD & 1BBq in 54 separate
8 transactions. Each of those transactions was funded by multiple bitcoin addresses associated with Silk
9 Road. In total, 1BAD & 1BBq were funded by approximately 3,056 sending addresses. This figure can
10 be obtained by looking at the number of sending addresses for each of those transactions in any
11 blockchain explorer or blockchain analytics software, all of which is publicly available information. Of
12 the 3,056 sending addresses, 3,014 were deposit addresses for Silk Road users. I determined this by
13 having an IRS-CI analyst compare each of the 3,056 addresses with the addresses stored in the data from
14 the seized Silk Road servers. This means that 98 percent of the sending addresses that funded 1BAD &
15 1BBq and therefore 1HQ3, were addresses used by Silk Road users to purchase drugs and other illicit
16 goods and services. The remaining 42 addresses were likely “change addresses,” which is equivalent to
17 the change one would receive in a monetary transaction and from which associations can also be made
18 using Reactor.

19 25. In short, before they were stolen and moved to 1BAD and 1BBq, the seized 69,370 BTC
20 were located in wallets that were subsequently seized and forfeited by the government in the criminal
21 prosecution of Ross Ulbricht.

22 **E. Consensus Among Blockchain Analytics Companies Regarding the Source of the Seized**
23 **69,370 Bitcoins**

24 26. The consensus among blockchain analytics companies like DMG was that the bitcoin at
25 issue here originated from Silk Road.

26 27. On or about November 4, 2020, the day after the Government’s seizure of the bitcoin at
27 issue and a day before the Government announced the seizure, Elliptic Co-Founder and Chief Scientist
28 Dr. Tom Robinson wrote, “...through blockchain analysis we can determine that these funds likely

1 originated from the Silk Road.” ([https://www.elliptic.co/blog/1-billion-silk-road-bitcoins-are-on-the-](https://www.elliptic.co/blog/1-billion-silk-road-bitcoins-are-on-the-move)
2 move).

3 28. Similarly, on or about November 4, 2020, blockchain analytics company CipherTrace
4 issued a similar article that stated in part, “On November 3, more than 69,370 BTC originating from the
5 Silk Road – one of the first darknet markets – moved for the first time since April 2015...”
6 (<https://ciphertrace.com/nearly-1b-from-silk-road-move-for-first-time-since-2015/>).

7 29. Lee’s conclusion that “the blockchain transactions show that the Bitcoins came from 58
8 sources” is surprising to me in light of his access to blockchain analytics tools and the fact that the origin
9 of the bitcoin at issue here is clear to so many major blockchain analytics companies who have
10 conducted a similar analysis.

11 **F. Silk Road’s “Bitcoin Tumbler”**

12 30. Claimants state that there is a disconnect between the tracing of the bitcoins in 1HQ3 to
13 “proceeds of criminal activity by Silk Road and Ulbricht” and that Silk Road used a tumbler to
14 obfuscate the payments it received from the sale of drugs and other illicit goods and services. *See*
15 Declaration of Rees Morgan, Dkt. No 98-6 ¶ 8(c) (“Morgan Declaration”). There is no disconnect
16 between these two things. Payments going into Silk Road were tumbled so that they could not be traced
17 to a particular user when bitcoin was withdrawn from the site. This approach was not very effective,
18 however, because any bitcoin coming out of the site could still be linked to the Silk Road website, the
19 sole purpose of which was to sell illicit goods and services. For example, if a buyer wanted to purchase
20 heroin from a Silk Road vendor, the buyer would send bitcoin to a bitcoin address assigned to the
21 buyer’s account but controlled by Silk Road. The buyer’s account would be credited with the requisite
22 amount of bitcoin. The buyer would use that credit to purchase heroin from the vendor. The actual
23 bitcoin received by the vendor was not the same bitcoin the buyer used to fund his account. This is what
24 Silk Road advertised as “tumbling;” however, all of the bitcoin was tainted because it all came from
25 individuals wishing to purchase illicit goods or services.

26 31. Attached hereto as Exhibit 3 is a Wall Street Journal article dated February 24, 2015
27 titled “Silk Road Mastermind’s Bitcoin Trail Wasn’t Complicated.” The article documented an
28 interview of Ilhwan Yum, a former FBI Special Agent who tied Ross Ulbricht to Silk Road through the

1 bitcoin money trail. The article references the bitcoin tumblers the Silk Road marketplace used “to
2 mask the origin and destination of transactions conducted on the network.” In the interview, Yum stated
3 that he did not “‘tumble’ his own transactions moving money out of the network, making it simple to
4 establish the connection between Mr. Ulbricht and Silk Road.” According to Yum, tying Ulbricht to
5 Silk Road through the bitcoin money trail “didn’t take any complicated analysis.” As the article notes,
6 although Ulbricht “may have had a complicated network to hide transactions within the Silk Road
7 marketplace, [] his extraction of funds from the network was easy to spot.”

8 32. Yum was also involved in the FBI seizure of servers and bitcoins that linked Ulbricht to
9 Silk Road. Yum testified at Ulbricht’s trial that he personally transferred the bitcoin linked to Ulbricht
10 to a government bitcoin address. During the trial, Yum “tracked the transactions from Silk Road to
11 [Ulbricht’s] laptop wallet.” According to Yum, those transactions were not tumbled, likely because
12 Ulbricht thought nobody would know who was linked to the address itself. Yum added: “Among the
13 bitcoin he received to his laptop, over 88% of those transactions weren’t tumbled. They were sent
14 directly from the marketplace to his wallet.”

15 I declare under penalty of perjury that the foregoing is true and correct to the best of my
16 knowledge and belief. Executed this 24th day of August 2021 in East Lansing, Michigan.


17
18 
19 JEREMIAH HAYNIE
20 Special Agent
21 Internal Revenue Service – Criminal Investigation
22
23
24
25
26
27
28

EXHIBIT 1

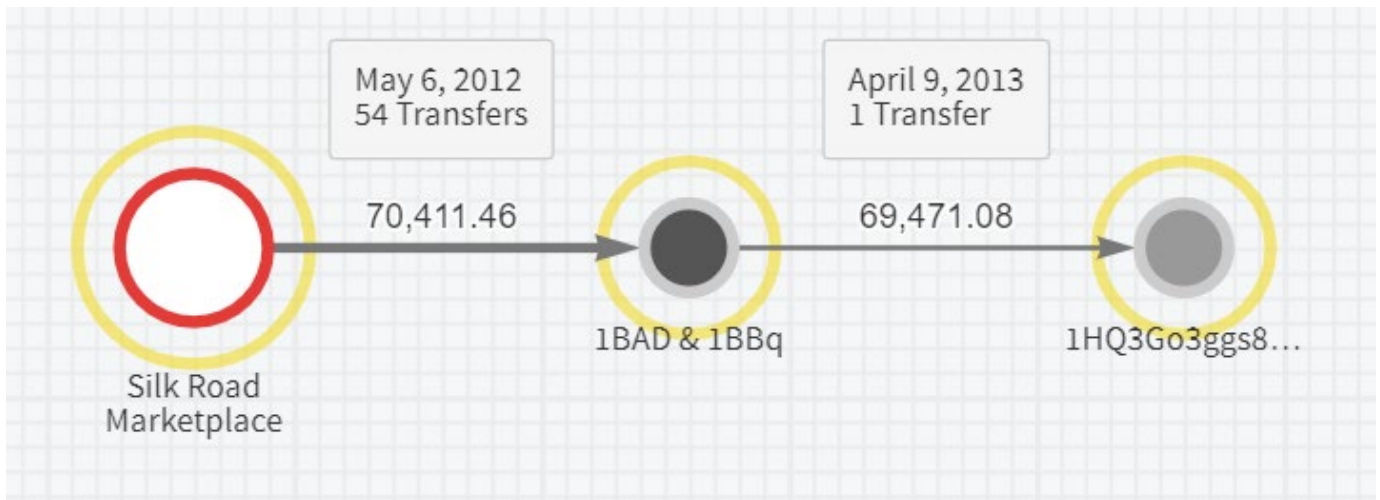


EXHIBIT 2

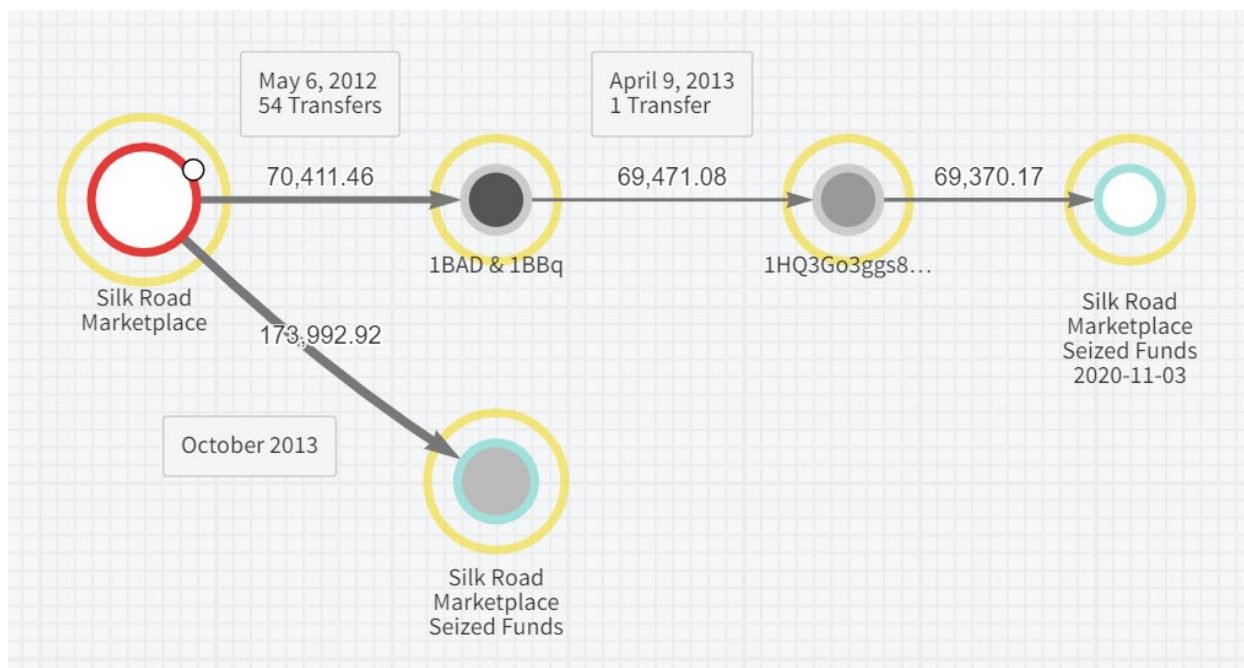


EXHIBIT 3

Silk Road Mastermind's Bitcoin Trail Wasn't Complicated

Dow Jones Institutional News

February 24, 2015 Tuesday 8:39 PM GMT

Copyright 2015 Factiva®, from Dow Jones
All Rights Reserved

FACTIVA®

Copyright © 2015, Dow Jones & Company, Inc.

 **DOW JONES NEWSWIRES**

Length: 1007 words

Byline: By Samuel Rubinfeld

Body

Ross Ulbricht, the convicted administrator of darknet marketplace Silk Road, was depicted as a criminal mastermind, but it was relatively easy for a cybercrime expert to follow his transactions.

Ilhwan Yum, a senior director in the litigation consulting group of FTI Consulting, testified in Mr. Ulbricht's trial. In his testimony, Mr. Yum described his role in the Silk Road investigation, laying out how he, then as an agent in the New York office of Federal Bureau of Investigation, tied Mr. Ulbricht to the network through the bitcoin money trail, though he admitted it didn't take any complicated analysis.

Prosecutors said the Silk Road marketplace used a "bitcoin tumbler" to mask the origin and destination of transactions conducted on the network. But Mr. Yum didn't "tumble" his own transactions moving money out of the network, making it simple to establish the connection between Mr. Ulbricht and Silk Road, he said in an interview following Mr. Ulbricht's conviction. In other words, Mr. Ulbricht may have had a complicated network to hide transactions within the Silk Road marketplace, but his extraction of funds from the network was easy to spot.

Mr. Yum was also involved in the FBI seizure of servers and bitcoins that linked Mr. Ulbricht to the marketplace, testifying at Mr. Ulbricht's trial that he personally transferred the bitcoin linked to Mr. Ulbricht to a government bitcoin address.

Mr. Yum discussed his role in the investigation and explained the bitcoin trail in an interview with Risk & Compliance Journal. The conversation has been lightly edited for context.

The Silk Road case involved undercover agents exposing a marketplace located on the dark Web involving a currency not exactly recognized by the government. How does that process even begin?

The case was looked at by other agencies prior to my former FBI squad. We only specialized in computer intrusions. There was a criminal act going on, so it wasn't much that we were targeting bitcoin. It was a criminal enterprise, and it just so happened they chose bitcoin as their payment method.

What is a bitcoin blockchain?

Silk Road Mastermind's Bitcoin Trail Wasn't Complicated

It's an open book on every transaction that occurs with bitcoin. I think most people understand that it's not truly anonymous any more. I think a lot of people mix up bitcoin, and the concept of anonymity. Bitcoin itself is just a string of numbers and letters; the parties behind the transactions are hard to identify. The beauty of bitcoin is the blockchain helps every transaction seem legitimate. At the same time, you're announcing every transaction conducted in bitcoin, which makes laundering more difficult.

A lot of people compare bitcoin to virtual cash. Cash transactions are hard to track, but imagine if every serial number [on a bill] used in a transaction was recorded and announced to the public. Limited to that alone, you can't track who made the transaction, but you can see a transaction happened.

What is a bitcoin tumbler and how does it exploit the bitcoin blockchain?

There are different ways to tumble things and different sites that promote their way of tumbling. What it does is it generates additional transactions, or ancillary transactions, in order to obfuscate what's being announced to the blockchain. It mixes your transactions with another transaction, making it hard to follow the money trail on the blockchain.

Why would someone use a tumbler?

You would use a tumbler if you realize bitcoin transactions don't have enough anonymity, and you don't want that address coming back to you. A [bitcoin] address is linked to an individual.

Is there a legitimate use for a tumbler?

If you truly valued your privacy, you could justify it. Regardless of the intention, the act itself can be considered money laundering. You may value your privacy but if you're trying to hide the source or trail of money, you're engaging in money laundering. I'm not a lawyer, though.

How did you crack the Silk Road tumbler's code?

The bitcoin transactions were supporting evidence [in the case]. We identified what he was doing on the marketplace. Our focus wasn't trying to crack the tumbler. In general terms, his tumbling wasn't as complicated as advertised. By that, I mean his method and logic of trying to mix the transactions. The exact detail of this, however, I can't get into.

Another example: During the trial, FTI, myself and a colleague of mine, we tracked the transactions from Silk Road to his laptop wallet. Those transactions weren't tumbled. If you go with the concept, you only know the transactions if you know the real-life link to that address. I can only assume Dread Pirate Roberts didn't bother to tumble it because he thought no one would know who was linked to the address itself.

Among the bitcoin he received to his laptop, over 88% of those transactions weren't tumbled. They were sent directly from the marketplace to his wallet.

Do you expect to see cases like this in the future?

Yeah, I think so. As you have seen in the news, almost right after Silk Road 1 was taken down, Silk Road 2.0 sprouted up. Silk Road 2.0 was taken down several months ago.

There are plenty of other marketplaces that serve as alternatives to Silk Road. They're all still using virtual currencies. They're getting better at the underlying technology behind bitcoins, and on how to obfuscate transactions. If your tumbling is successful in the middle of a transaction, you might be able to figure out who is sending and who is receiving money, but you can't really have a solid link or money trail. If you are the organization behind the tumbler, you can see the trail. But without the back end, it's hard to track.

Write to Samuel Rubinfeld at Samuel.Rubinfeld@wsj.com Follow him on Twitter @srubinfeld.

Silk Road Mastermind's Bitcoin Trail Wasn't Complicated
